Sub B1

storing the data as encrypted data element values (DV) in records (P) in a first database (O-DB), each data element value being linked to a corresponding data element type (DT)[,]; [characterized by the steps of]

storing in a second database (IAM-DB) a data element protection catalogue [(DC)] (DPC), which [for] contains each individual data element type (DT) [contains] and one or more protection attributes stating processing rules for data element values (DV), which in the first database (O-DB) are linked to the individual data element type (DT)[,];

C2 cont

for each user-initiated measure aiming at processing of a given data element value (DV) in the first database (O-DB), initially producing a [compelling] calling to the data element protection catalogue for collecting the protection attribute/attributes associated with the corresponding data element type, and

[compelling] controlling the user's processing of the given data element value in conformity with the collected protection attribute/attributes.

C3

4. (Twice Amended) A method as claimed in claim 1, wherein the encryption of data in the first database (O-DB) and/or the encryption of data in the second database (IAM-DB) is carried out

27

C

C3 cont.

in accordance with [the PTY] a PROTEGRITY principle with floating storage identity.

Sub B2

8. (Amended) An apparatus for processing data that is to be protected, comprising:

a first database (O-DB) for storing said data as encrypted data element values (DV) in records (P), each data element value being linked to a corresponding data element type (DT)[, characterised by];

C4

a second database (IAM-DB) for storing a data element protection catalogue [(DC)] (DPC), which [for] contains each individual data element type (DT) [contains] and one or more protection attributes stating processing rules for data element values (DV), which in the first database (O-DB) are linked to the individual data element type (DT)[,];

means which are adapted, in each user-initiated measure aiming at processing a given data element value (DV) in the first database (O-DB), to initially produce a [compelling] calling to the data element protection catalogue for collecting the protection attribute/attributes associated with the corresponding data element types, and

C4 cont Sub B2

means which are adapted to [compellingly] control the user's processing of the given data element value in conformity with the collected protection attribute/attributes.

Please add the following new claims:

Sub B3

--9. A method for processing of confidential data comprising the steps of:

providing a first database (P-DB), a second database (O-DB), and a third database (IAM-DB);

entering descriptive information (DI) with certain portions of the descriptive information being classified as certain data types (DT) of a plurality of different data types;

assigning an initial identity (OID) to the descriptive information;

CS

storing a first record in the first database including in the initial identity;

encrypting the initial identity to form a storage identity (SID);

accessing a catalogue (DCP) of encryption protection degrees in the third database, the catalogue including encryption levels for each of the different data types;

encrypting the certain portions of the descriptive information in accordance with their data types; and

C

storing a second record in the second database including the storage identity and the encrypted descriptive information (DV).

15 ~~10.~~ The method according to claim 9, wherein the first record is not encrypted.

16 ~~11.~~ The method according to claim 15 ~~10~~, wherein the first record includes an individual's name and address.

10 ~~12.~~ The method according to claim 9, wherein the third database is physically separate from the second database.

17 ~~13.~~ The method according to claim 16 ~~11~~, wherein the different data types represent different types of personal data corresponding to the individual.

11 ~~14.~~ The method according to claim 9, wherein said step of encrypting the initial identity to form the storage identity includes a non-reversible encryption followed by a reversible encryption.

12 ~~15.~~ The method according to claim 9, wherein the catalogue of encryption protection degrees in the third database is encrypted.

13 ~~16.~~ The method according to claim 9, wherein the catalogue of encryption protection degrees includes encryption rules for encrypting the different data types.

14 ~~17.~~ The method according to claim 9, wherein the catalogue of encryption protection degrees includes rules for which program or programs may manage the different data types.--

REMARKS

Applicant thanks the Examiner for the very thorough consideration given the present application.

Claims 1-17 are now present in this application. Claims 1, 8 and 9 are independent. Claims 1, 4 and 8 have been amended, and claims 9-17 have been added in order to more clearly recite the novel and inventive features of the present invention.

Reconsideration of this application, as amended, is respectfully requested.

C